Secure Data Collection and Critical Data Transmission Technique in Mobile Sink Wireless Sensor Networks

Thesis submitted in partial fulfillment

of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Deepak Puthal

(Roll No: 210cs2209)

Department of Computer Science and Engineering

National Institute of Technology, Rourkela

Rourkela-769 008, Orissa, India

2012

Secure Data Collection and Critical Data Transmission Technique in Mobile Sink Wireless Sensor Networks

Thesis submitted in partial fulfillment

of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Deepak Puthal

(Roll No: 210cs2209)

under the guidance of

Prof. Bibhudatta Sahoo

Department of Computer Science and Engineering

National Institute of Technology, Rourkela

Rourkela-769 008, Orissa, India

2012

Dedicated to my family

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India.

Certificate

This is to certify that the work in the thesis entitled ***"Secure Data Collection and Critical Data Transmission Technique in Mobile Sink Wireless Sensor Networks"*** submitted by ***Deepak Puthal*** is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology with specialization of Information Security in the department of Computer Science and Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT, Rourkela
Date: 04 June 2012

Prof. Bibhudatta Sahoo
Assistant Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Acknowledgment

First of all, I would like to express my heartfelt thanks to my guide, Prof. Bibhudatta Sahoo for giving me the guidance, encouragement, counsel throughout my research and painstakingly reading my reports. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis. His wide knowledge and logical way of thinking have been of great value for me. As a guide he has a great influence on me, both as a person and as a professional.

I would like to express my gratitude to Dr. Ashok Kumar Turuk and Dr. B. Majhi, who was constant source of encouragement to me and helping me with his insightful comments on all stages of my work. Dr. Pankaj kumar Sa is like a constant source for me from beginning at the department. His help can never be expressed in words.

I am indebted to Prof. S. K Rath, Prof. S. K Jena, Dr. D. P. Mohapatra, Dr. P. M. Khilar and all other faculties of Department of Computer Science and Engineering for their guidance throughout my study at NIT Rourkela. And also I express my gratitude to Suraj Sharma for generously sharing his time and knowledge and for making me fun while working, just like a friend.

I would like to express sincere thanks to Dr. Bheemarjuna Reddy Tamma for his excellent guidance, invaluable suggestions and continuous encouragement towards research during summer Internship at IIT Hyderabad. He has helped me to learn a lot of research areas in networking. I am lot of indebted to him.

Finally, I am forever indebted to my family for their understanding and encouragement when it was most required. Such a connection is valuable in itself.

Deepak Puthal

deepakpnitr@gmail.com

Abstract

In Mobile sink wireless sensor networks (MSWSN) Sensor nodes are low cost tiny devices with limited storage, computational capability and power except the sink node. Mobile sink has no resource limitation. It has wide range of application in the real world problem like military and civilian domain etc. The nodes in the network are unattended and unprotected so energy efficient and security are two major issues of sensor network. The sensors have limited battery power and low computational capability, requires a security mechanism that must be energy efficient. In this proposed system model mobile sink traverse the network to collect the data.

Here we proposed energy efficient secure data collection techniques with mobile sink wireless sensor networks based on symmetric key cryptography. In proposed data collection technique mobile sink traverse network and collect data from one hop neighbors. Proposed cryptosystem is time based as after each fixed amount of time sink generates a large prime number. Using the prime number all nodes in the network update their key to avoid replay attack keep. Data collection MSWSN is three step process. At each new position mobile sink broadcast a beacon frame to alert the static sensors about its presense, secondly sensors send their sensed data towards sink node and finaly mobile sink broad cast another beacon frame to stop the data transmission by sensors. Sensor authenticate the mobile sink with the shared key concept, if it finds that sink is the legitimate node then sensor encrypt their data and transmit it to the sink.

A static sensor sense some critical information and sink is not within its range, that that time sensor needs to transmit its data towards sink immediately. It cannot wait till sink come to its range. For that we proved an existing protocol Sensor Protocol for Information via Negation (SPIN) is efficient for critical data transmission to the mobile sink. Then we make it as the secured protocol by using symmetric key cryptography. Here we use the previous assumption to make it as the secure protocol.

All the simulation has been carried out with NS 2.34. This thesis is supported by

the literature survey in the area of Mobile Sink Wireless Sensor Networks to make it complete.

Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Description
WSN	Wireless Sensor Networks
MSWSN	Mobile Sink Wireless Sensor Networks
GIT	Greedy Incrimental Tree
SPIN	Sensor Protocol for Infromation via Negotiation
CAC	Central Authentication Code
SAC	Sensor Authentication Code
MAC	Message Authentication Code
CDMA	Code Division Multiple Access
MSs	Mobile Sinks
MDCs	Mobile Data Collectors

Chapter 1

Introduction

Introduction

Mobile Sink Wireless Sensor Networks

Motivation

Problem Statement and Objectives

Organization of the Thesis

1.1 Introduction

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data. Some of the popular applications of sensor network are area monitoring, environment monitoring (such as pollution monitoring), industrial and machine health monitoring, waste water monitoring and military surveillance.

Sensor networks are predominantly data-centric rather than address-centric. So sensed data are directed to an area containing a number of sensors rather than particular sensor addresses. Aggregation of data increases the level of accuracy and reduces data redundancy. A network hierarchy and clustering of sensor nodes allows for network scalability, robustness, efficient resource utilization and lower power consumption.

In Mobile Sink Wireless Sensor Networks (MSWSN) all sensors are static other than the sink node. Mobile nodes are the destination of messages originated by sensors, i.e., they represent the endpoints of data collection in the network. They can either autonomously consume collected data for their own purposes or make them available to remote users by using a long range wireless Internet connection. In [34] sensor nodes are static and densely deployed in the sensing area. One or multiple Mobile sinks (MS) move throughout the network to collect data from all sensors. Communication between the source sensors and the MS is either single hop or multi-hop.

The amount of data that can be collected over a long period of time is depending

on the maximum data storage capacity of a sensor node and the battery lifetime of the sensor [44]. If data is collected at a rate that exceeds the storage capacity of the node during the expected battery lifetime of the unit, then the node must be retrieved prior to full battery expenditure or the data must be transmitted to another location. In the latter case, the energy cost of transmitting the data must be taken into account when determining the deployment time of sensor nodes. Data collection method is of two types i) proactively and ii) reactively. In proactive method sensed data distributed periodically distributed throughout the network and mobile sink retrieved it later. In reactive data collection method sensors send their data towards the mobile sink as a reaction for the detection of sinks queries.

During the data collection technique in mobile sink sensor networks, security is an important factor. Node need to be authenticate before start the data collection process. At the same time sensors also need to authenticate the sink. After authentication takes place the start the data communication process with specified rule. During the data collection sensor send their data with encrypting the data packets and send it to the sink node. When sink receive the data it decrypt the packet and check for the adversary modification during data transmission. This node authentication, data encryption and decryption use different cryptography technology. Using cryptography function it secure the communication process.

1.2 Mobile Sink Wireless Sensor Networks

In Mobile Sink Wireless Sensor Networks all the sensors are statically deployed to sense the environment and mobile sink traverse the networks. It overcomes the problem of the sink neighborhood problem as defined in previous section [31]. In the sink neighborhood problem is neighbor nodes of sink participate more in the data transmission. The result is the faster energy deplete compared to other nodes in the network. If we look over the energy conservation model sensor deplete some amount of energy during the data receiving and the data transmission. As the sensor those are close to the sink, participate more data transmission i.e. for them and for those sensors away

from the sink in the same direction.

In MSWSN all nodes are static other than the sink in the network. Mobile sink traverse randomly to collect the sensor data. It may be collect with one hop or multi hop communication and our proposed model is the one hop data collection. As sink traversing throughout the network for data collection so the neighbor of the sink is not fix, so neighborhood problem will not arises. Here we use LR-WPAN IEEE 802.15.4 low cost wireless link. IEEE 802.15.4 intends the lower network layers of a type of wireless personal area network (WPAN) which focuses on low cost, low speed global communication between the sensors. IEEE 802.15.4 security consists of four kinds of security services such as access control, message integrity, message confidentiality, and replay protection [47]. The access control feature should prevent illegal users to participate in the process. In other word, only authorized users can able join in a legitimated network. Message integrity means the validity of transferred data and message authentication implies message sender's verification using cryptographic function. These message integrity and message authentication are possible using message authentication code(MAC) in IEEE 802.15.4. The MAC is appended to each data packet sent [48].

A malicious node can participate in the data collection process by showing it as the sink node. Then all the sensed data collected by the malicious node, for that we need to authenticate the node before sending the sensed data. If sensors send its packets without encryption then malicious node can accept the packet then it can modify the content of the packet. So we'll lose the original content of the data. Data is neither to be modified nor be dropped. We need to keep data freshness. For that we need to use cryptography concept to secure the data collection technique. The security requirements of mobile sink sensor networks and the attacks possible in each layer are described in Section 2.6.

1.3 Motivation

In Wireless Sensor Networks (WSN), there are several challenges. The main challenges are how to maximize network life time and how to provide secure communication

in the network. As sensor network totally rely on battery power, the main aim for maximizing lifetime of network is to reduce battery power conservation or energy with some security considerations. In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. It is said in [4] that 70 percent of energy consumption is due to data transmission. As sensor network generally deploied in hostile environment so security is the major issue in the network.

Major operation takes place in the sensor network is to monitoring the environment and send the monitored data to the sink node. In case of static sensor networks all sensors are static with the sink node. When the data communication takes place all the static sensors send their sensed data to the sink which is fare away from the sensors. In that situation those sensors are close to the sink; participate more times in the data transmission than the other sensor. The result is to deplete their energy faster than the other nodes, the premature disconnection of the networks [34]. So sink got isolated from the network, while all other nodes are fully operational along with the sink. This problem, here termed the "sink neighborhood problem," leads to a premature disconnection of the network. With the data collection process sink gets the data from the sensors. During data collection node may be participate in the process and drop the packets. With this process sink need to be authenticate the node, encryption and decryption of the data [8][14][16][28]. Here one energy efficient data collection technique is proposed with Mobile Sink Wireless Sensor Networks. We proposed the random relative motion of the sink to collect data and reduce energy conservation and tp prolong network life time. Cryptographic technique is used for node authentication and data encryption. Our motivation for proposing an energy efficient data collection technique and reduce the packet drop. Use cryptographic method for secure data collection with node authentications.

In MSWSN, sink traverse the network for data collection. Sensor networks generally deployed in hostile environments. So sensor may sense any critical data or highly sensitive data. In such situation it can't wait till the time sink come into its range and it'll send its data to sink [34][36][45]. It needs to deliver the data towards mobile sink

immediately. As it's a high sensitive data so we need to encrypt the data to avoid the external attack [32].

1.4 Problem Statement and Objectives

We propose a framework to establish secure energy efficient data collection with mobile sink. So that data can be collected as a secure manner and prolong network lifetime.

Sensor networks are usually deployed in hostile and unattended environment where an adversary can read and modify the content of the data packet. For such situation the most popular type of attack is the external attack and replay attack. Node need to be authenticate before data transmission takes place. Network life time is also an important issue in sensor networks. In external attack the node does not belong to the network try to read and modify the packet. If node read and modify the packet sink will not get the correct data. For that we also need to authenticate the node before data transmission. We use concept of mobile sink to prolong network lifetime and overcome the sink neighborhood problem.

In mobile sink sensor networks, sink traverse the network to collect data. If a node sense some critical data and sink is not its range, for that situation sensor node transmit the data to mobile sink immediately. For that we proved an existing protocol for critical data transmission and make it as the secure protocol to avoid external attack and node authentication during data transmission.

Securely collect the data from network and critical data transmission to mobile sink in mobile sink sensor networks. Accordingly we identify the objectives of the thesis and list them as follows:

- Energy efficient data collection method
- Symmetric key based secure communication
- Protocol for critical data transmission to mobile sink
- Secure Protocol for critical data transmission to mobile sink

1.5 Organization of the Thesis

In this chapter, the motivation for secure and energy efficient data collection technique, the objectives of our work is discussed in a briefly. The organization of the rest of the thesis and a brief outline of the chapters in this thesis are as given below.

In chapter 2, we have discussed about the proposed system model and sink mobility model of mobile sink sensor networks. We also have discussed the data collection with mobile element and then performance metrics. We addressed the security requirement and the layer wise attack possible in MSWSN.

In chapter 3, we have described our proposed energy efficient data collection technique in mobile sink wireless sensor networks with one hop communications and applied symmetric key cryptography for secure data collection. Then, we have analyzed and checked the performance by simulating the proposed technique.

In chapter 4, we have proved that Sensor Protocol for Information via Negotiation (SPIN) is suitable for critical data transmission towards mobile sink. We use symmetric key cryptography for secure data transmission to mobile sink. We implement the proposed technique and analyze the performance and security.

Finally, chapter 5, summarizes the main contributions of this thesis and comments on future directions for this work.

Chapter 2

Mobile Sink Wireless Sensor Networks: Model, Performance Metrics and Security Issues

Introduction

System Model

Mobility Model of Sink

Wireless Sensor Networks with Mobile Data Collector

Performance Metrics

Security Issues

Conclusion

2.1 Introduction

Securing WSN is a challenging task because of its properties and characteristics such as unreliable wireless communication, resource constraints and unknown topology with earlier deployment, physical tampering of nodes due to unattended environment. To secure them, we have to satisfy security goals. These security goals can be classified into primary and secondary based on their importance. The primary security goals are data confidentiality, integrity, availability and authenticity. The secondary goal which has least importance than primary is data freshness, self-organization, time synchronization and secure localization. These primary goals are required based on the application for WSN [39].

WSN are easily disposed to security attacks due to its deployment in hostile environment. Although, there are many security solutions for traditional networks. They are not suitable for WSN due to its open space deployment and resource constraints, memory and energy. Because of which nodes cannot do complex computations and store large data. So, there is a need to find new security measures which will be best suitable for the sensor networks. MSWSN is one of the solution for prolong network life time and overcome all the attacks possible in multi-hop communication. Before discussing about our problem, we are going to discuss about the Mobile Sink Wireless Sensor Network, its system model, sink mobility model, security threat models and layer wise attacks in WSN.

2.2 System Model

The proposed system model is single hop data collection by mobile sink node in MSWSN. Data collection means get the data from the sensors. In Table 2.1 it is defined the configuration of simple sensor node. Its application is like in betel field or military applications. More specifically it is applicable in flat region because sink travers the network to collect the data.

We brought the random graph theory into modeling a class of sensor networks with low sensor density in this thesis. Consider the following situation. An area

covered with a great deal of sensor nodes that form a sensor network $G(V,E)$ through self-organization, where V stands a set of all sensors and E stands a set of all existing communication connections. Monitored area covered by the sink node's range of a certain task is a subset of $G(V,E)$, we denote it by $G_i(V_i,E_i)$. Here we consider a set S_i, which contains the vertices (Sensors) V_i.

A random graph consists of vertices and edges. Any two vertices share an edge with the same probability p. The probability of a random graph being connected tends to 1, if E is greater than $\mathrm{P_C(E)} = \frac{\mathrm{N/log}N}{2}$ (N is the number of vertices and E is the number of edges). This is what we call a 'phase transition' in random graphs that implies a sudden large change of network performance at P_c. In other words, the value of P_c is a threshold beyond which the random graph is 'connected'.

Mapping random graphs to sensor networks is unrealistic. But in our model connections establishes between sensors and sink, not between the sensors. Link establishes when sensor finds that sink is in its one hop range.

2.2.1 Assumptions

Assumption 1: For convenience of simulation we assume that G_i is an area covered by the sink node with its one hop transmission range.

Assumption 2: G_i is covered with the same sensors (homogenous sensors), which implies that each sensor has the same communication radius including sink node.

Assumption 3: We call G_i transfer the data to the sink after finding its presence within its range. Data transmission takes place with one hop communication between sensor and sink.

Assumption 4: We assume that the sink has no resource limitation, i.e. computational, memory and energy.

2.2.2 Network Structure

Sink node at $N(i,j)$ only have four candidates of edges with sensors ($N(i-1,j), N(i+1,j), N(i,j-1), N(i,j+1)$) that are in square lattices adjoining $N(i,j)$ in Figure 2.1 Like

CPU	8-bit, 4 MHz
Storage	8K Instruction flash, 512 bytes RAM, 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10 Kilobits per second
Operating System	TinyOS
OS code space	3500 bytes
Available code space	4500 bytes

Table 2.1: Basic configuration of a simple sensor node

this way all the nodes are connected with the sink node, those are within its one hop range.

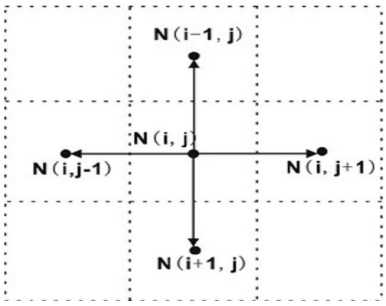

Figure 2.1: Sink and four sensors in its range represent as edge.

We consider a large n number of fixed homogenous sensor nodes placed uniformly according to sensors range in a square region given by a geographical area, for sensing data or monitoring events. Single mobile sink travels in the squared monitored region to collect data by one hop communication [31]. It follows the proposed mobility model to traverse the network to collect data, described in next session. Sink collects the data from the sensors; those are one hop range from the sink shows in Figure 2.2. Here we follow the one hop data collection to avoid the threats arrises in multi hop data data collections. There are two types of data collection; one is proactive data collection and another is reactive data collections. In proactive data collection method sensed data distributed and store throughout the network for later retrieval of mobile sink. In reactive data collection method data send to the sink after detection of sinks presence

or query. Our model follows the reactive data collection.

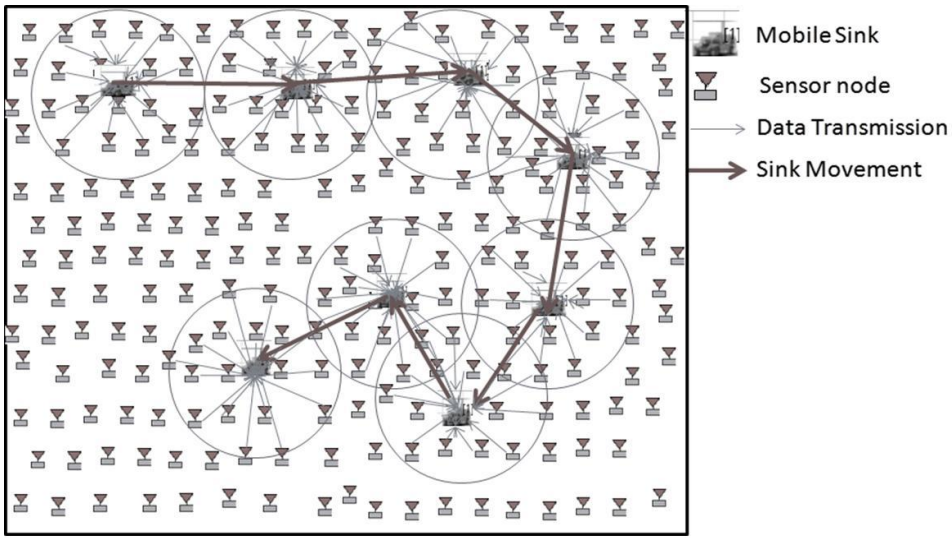

Figure 2.2: System model for Wireless Sensor Networks with Mobile Sink.

The network has 'n' number of fixed homogenous sensor nodes. At each position of sink the k_i number of sensors covered by sink's range at time t_i with connected graph $G_i(V_i, E_i)$.

So at time t_1 sink covers k_1 number of sensors with set s_1.

At time t_2 sink covers k_2 number of sensors with set s_2.

With our proposed random relative mobility model the inter section if two consecutive set will not be empty.

$$s_1 \cap s_2 \neq \phi$$

generally, $s_i \cap s_j \neq \phi$, where i and j are two consecutive number.

Two consecutive set intersections should not be empty because in this model sensors send their data to the sink with one hop distance, only when the sink is within their range. If we omit some sensor within two consecutive position, those sensors unable to send their data to the sink. Our main aim is to collect the data from all sensors.

2.3 Mobility Model of Sink

Our proposed mixed mobility model which is the combination of random way point and modified Gauss-Markov model [31]. Gauss-Markov mobility model is initially proposed for PCS [33]; and this model has been used for an ad hoc network protocol. Here we describe how it works for mobile sink in the MSWSN.

2.3.1 Modified Gauss-Markov Model

Assume that at time t_1 sink is at position $p_1(x_1, y_1)$.
Initially it needs to specify the position of the sink. Then it starts movement with the based on previous position, speed and direction. At the n^{th} position:

$$\begin{aligned} x_n &= x_{n-1} + s_{n-1}\cos(d_{n-1}) \\ y_n &= y_{n-1} + s_{n-1}\sin(d_{n-1}) \end{aligned} \tag{2.1}$$

Where (x_n, y_n) and (x_{n-1}, y_{n-1}) are the current and the previous position of the sink node respectively. s_{n-1} and d_{n-1} are the speed and direction of the previous (x_{n-1}, y_{n-1}) position.
The Gauss-Markov Mobility Model was designed to adapt to different levels of randomness. More specifically, the value of speed and direction at the n^{th} instance is calculated based upon the value of position, speed and direction of the $(n-1)^{th}$ instance and a random variable shown in the following equations:

$$s_n = \alpha s_{n-1} + (1-\alpha)s' + \sqrt{(1-\alpha^2)}s_{xn-1} \tag{2.2}$$

$$d_n = \alpha d_{n-1} + (1-\alpha)d' + \sqrt{(1-\alpha^2)}d_{xn-1} \tag{2.3}$$

Where s_n and d_n are the new speed and direction of the sink at time interval n, s′ and d′ are constants representing the mean value of speed and direction as $n \to \infty$; $0 \leq \alpha \leq 1$, is the tuning parameter used to vary the randomness, and s_{xn-1} and d_{xn-1} are random variables from a Gaussian distribution. As the proposed model's assumption is the random motion of the mobile sink, so that it is according to values of α, s_{xn-1} and d_{xn-1} are taken randomly. Total random values obtained by setting $\alpha = 0$ and linear motion is

obtained by setting $\alpha = 1$. Intermediate levels of randomness are obtained by varying the value of α between 0 and 1.

When the sink reaches at the boundary, it returns back to the previous position. Therefore, each time the sink needs to save the previous position in order to calculate the next position and returns back when it heats the boundary.

2.3.2 Random Waypoint Mobility Model

This mobility model includes pause times between succesive position change. Here sink stays at a location for a certain period of time known as pause time. At each step sink node stays for a fixed amount of time. Once pause time expires, it moves towards the newly chosen position at the selected speed.

2.3.3 Mixed Mobility Model

Speed, direction and position is being calculated by Gauss-Markov model, whereas random waypoint only gives the pause time. Here we use pause time because sink needs to collect the packet/data before changing its position and here we have taken a long pause time of 20 second.

We implemented the proposed mixed mobility model for sink in MatLab and check the performance. It covers the maximum area within the specified region for data collection.

2.4 Wireless Sensor Networks with Mobile Data Collector

To better understand the features of Wireless Sensor Networks with Mobile Sink, let introduce the network architecture first, which is detailed according to the role of the mobile sink [34].

Sensor nodes (or just nodes) are the sources of information. Such nodes perform sensing

as their main task. They may also forward or relay messages to the network, depending on the agreed communication paradigm.
Sinks (base stations) are the destinations of information. It collects data sensed by sensor nodes either directly (i.e., by visiting sensors and collecting data from each of them) or indirectly (i.e., through intermediate nodes). They can use data coming from sensors autonomously or make them available to interested users through an Internet connection.
Special support nodes perform a specific task, such as acting as intermediate data collectors or mobile sink. They are neither sources nor destinations of messages, but exploit mobility to support network operation or data collection.

Note that sink might be mobile at the network. Depending on the specific scenario, the support nodes might be present or not. When there are only regular nodes, the resulting WSN with mobile sink architecture is homogeneous. Furthermore, different from traditional WSN, which are usually limited to be dense, WSN with mobile sink can also be sparse. As the network architecture strongly depends on the role of the mobile sink, we will analyze it in detail in the following section.

Mobile Data Collectors (MDCs). These are mobile elements which visit the whole network to collect data sensed by the sensors. Depending on the mobility of collector it manages the collected data.

Mobile Sinks (MSs). Mobile nodes are the destination of messages originated by sensors, i.e., they represent the endpoints of data collection in the network. They can either autonomously consume collected data for their own purposes or make them available to remote users by using a long range wireless Internet connection. In [34] ordinary sensor nodes are static and densely deployed in the sensing area. One or multiple Mobile sinks (MS) move throughout the network to gather data coming from all sensors. Note that the path between the source nodes and the MS is either single hop or multi-hop.

In [35] defined the application, people act as MSs by collecting environmental data (such as pollutants concentration and weather conditions) for their own purposes. The reference WSN scenario is represented by a sparse WSN where multiple MSs can be in

contact with a single sensor node at the same time.

Mobile Relays (MRs). These are intermediate nodes which gather data from sensors, store them, and carry the collected data to sinks or base stations. They are not the endpoints of communication, but only act as mobile forwarders. This means that the collected data move along with them, until the MRs get in contact with the sink or base station. Here the sensors and sink are static and only relay node is movable.
So data collection is of two types one type is proactive another is reactive [46].

- **Proactive:** In this type of data collection method monitored data is distributed and stored throughout the network for later retrieved by the mobile sink.
- **Reactive:** In this type of data collection method data sent towards the mobile sink as a reaction for the detection of sink's presence or queries.

Here our data collection method follows the reactive data collection. It follows the one hop reactive based data collection.

2.5 Performance Metrics

2.5.1 Throughput/ Delivery Ratio

In Wireless Sensor Networks throughput is the average rate of successful message delivery over communication radio. This data may be delivered by the physical or logical link, or pass through certain network nodes. The throughput is usually calculated in bits per second (bps), and sometimes in data packets per second or data packets per time slot. Yuxi et al. [28] showed that lossy links do have significant impact on the maximum achievable throughput. There are some cases, where a network can achieve half of the throughput of the corresponding lossless network. Lossy links also affects energy efficiency. Lossy network can only achieve half of the throughput when links are lossless.

2.5.2 Network Life Time

Network lifetime is the key characteristic for evaluating sensor networks in an application-specific way. The lifetime of sensor network depends on the operation time of individual sensor nodes. Lifetime of wireless sensor networks ends when first node dies in the network. Y. Chen et al. [29] described two key parameters at the physical layer that affect the lifetime of the network: the state of the channel and the residual energy of sensors. Here in this letter they proposed a greedy approach to lifetime maximization which achieves considerable improvement in the lifetime performance.

2.5.3 Node Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to confirm that the data used for decision-making process must originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data is really sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

2.5.4 Data Freshness

In [30] Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness denotes that the data is recent, and it confirms that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering, but carries no

delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation [30]. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network [39].

2.6 Security Issues

In this section we classify the security requirement and the layer wise attacks possible in sensor networks. In this thesis we mainly focused on to avoid the external attack and node authentication during data collections.

2.6.1 Security Requirements

A sensor network is a special type of network. It shares some commonalities with traditional network, but also add some unique requirements of its own. Therefore, the requirements of a wireless sensor networks as including both the typical network requirements and the unique requirements suitable exclusively to wireless sensor networks.

Data Confidentiality

Data confidentiality is the most important issue in the wireless network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following [15, 16]:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In several applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

- Public information of sensor, such as sensor unique key and public keys, should also be encrypted to some extent to protect against trafic analysis attacks.

The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, to achieving confidentiality.

Data Integrity

With the implementation of confidentiality, an adversary may be incapable to take information. This doesn't mean the data is safe. The adversary can modify the data, so as to send the sensor network into disorder. For example, a malicious node may add some fragments or modify the data within a packet. Then this new packet can then be sent to the original receiver. Data loss or damage can also occur without the presence of a malicious node due to the exacting communication environment. Thus, data integrity ensures that any received data has not been altered during transmission [14].

Data Freshness

Even if confidentiality and data integrity are assured, we also need to take care of the each data freshness. Data freshness ensures that the data is recent, and it has no replayed of old messages by adversary node. This is especially required when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. It takes time for new shared keys to be distributed throughout the network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

Availability

Applying the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some methods take to modify

the code to reuse the code as much as possible. Some methods try to make use of additional communication technology to achieve the same goal. All these methods decline the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central processing scheme. This greatly threatens the availability of the network.

The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-behaving according to the situations. There is no fixed infrastructure available for the network management in a sensor network. This feature causes to brings a great challenge to wireless sensor network security. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors [17]. In order to apply public-key cryptography in sensor networks, an efficient mechanism for public-key distribution is necessary as well. In the same way the distributed sensor networks must self-organize to support multi-hop routing and to conduct key management and building trust relation among sensors. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be overwhelming.

Time Synchronization

Most sensor network applications based on the form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Further, sensors may compute the end-to-end delay of a packet as it travels between two consecutive sensors. For more collaborative sensor network may require group synchronization for tracking applications. In [24], the authors propose a set of secure synchronization protocols for sender-receiver (pairwise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to confirm that the data is using for any decision-making process originates from the authenticated source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

Adrian Perrig et al. propose a key-chain distribution system for their μTESLA secure broadcast protocol [16]. The basic idea of the μTESLA system is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys. In this case a sender will broadcast an encrypted message by using a secret key. After a certain period of time, the sender will disclose the secret key. The receiver is responsible for buffering the packet until the secret key has been disclosed. . After disclosure the receiver can able authenticate the packet and provided that the packet was received

before the key was disclosed. One limitation of μTESLA is that some initial information must be unicast to each sensor node before authentication of broadcast messages can begin.

2.6.2 Types of Attacks Possible in WSN

Regarding to the security of a WSN, it can be investigated in different perspectives, for example WSN attacks can be classified as two major categories: as external and internal attack according to the domain of attacks.

External attack: The attack is defined as the attacker does not belong to the network and it does not have any internal information about the network such as cryptographic information. In other word it can be defined as physical attack.

Internal attack: When a genuine node of the network act abnormally or illegitimate way, it considers as an internal attack. It uses the compromised node to attack the network which can destroy or disrupt the network easily.

Here in thesis we mainly focussed on to avoid the external attacks and authenticae the legitimate node during data collections. Here various types of attacks are defined layerwise [39].

Physical Layer

Jamming: Interference with the radio frequencies a network's nodes are using

Tampering: Physical compromise of nodes

Solutions: spread spectrum communication, jamming reports, accurate and complete design of the node physical package

Data Link Layer

Collision: Altering of transmission octets to disrupt the packets (checksum mismatch, back off in some MAC protocols)

Exhaustion: Collisions and back of in MAC protocols result in re-transmissions which result to the exhaustion of battery resources

Unfairness: Degrading service by causing users of a real-time MAC protocol to miss their deadlines

Interrogation Attack: Here attacker continuously sends RTS packets ignoring CTS packets and which results in flooding of packets in network links of targeted nodes.

SYBIL Attack: In one variation single malicious node act as different nodes and then gives many negative reinforcements to make the aggregate message a false one. In other way it stuffs the ballot box where sensor nodes take help of voting mechanism to choose a better link.

Solutions: Error correcting codes, collision detection and avoidance techniques, rate limiting.

Network Layer

Selective Forwarding: Malicious nodes refuse to forward certain messages and simply drop them

Sinkhole: The adversary attracts the surrounding nodes with unfaithful routing information

Sybil attack: A single node presents multiple identities to other nodes

Wormhole: The adversary tunnels the traffic received in a part of the network to another

HELLO flood: A laptop-class attacker broadcasts information with enough transmission power convincing every node in the network that he is his neighbor

Spoofing and alternating routing information: Adversaries node may be successfully creates routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end to end latency etc.

Node capture/Node replication attack: If an attacker can get physical access to the entire network, it can not only capture a node and copy cryptographic keys but also can launch replicated sensor with all captured cryptographic keys into strategic points in the network.

Solutions: Link layer encryption and authentication, multipath routing, identity verification, authenticated broadcast.

Transport Layer

Flooding: The adversary sends many connection establishment requests to the victim (memory and resource exhaustion)
DE synchronization: The adversary repeatedly forces messages which carry sequence numbers to one or both endpoints (request for retransmission of missed frames)
Solutions: packet authentication including all control fields in the transport protocol header.

2.7 Conclusion

In this chapter, we presented the system model of Mobile Sink Wireless Sensor Networks and random relative mobility model of mobile sink as a new paradigm for wireless Sensor Networks. We classify the security requirement and the layer wise attacks possible in mobile sink sensor networks. Here also we have addressed the performance metrics of the network. In the next chapter, we look for the new method for data collection from security view point, to avoid external attack and node authentication during data collection.

Chapter 3

Secure Data Collection using Symmetric Key Cryptography

3.1 Introduction

The proposed framework for data collections called data collection with mobile sink. This is relating components that can be used to design energy efficient secure method that are adaptive to the environment. One mobile sink is deployed in the network to collect the data from the sensors with one hop communications. All the sensors are fixed other than the sink node and sensors are deployed sparsely to sense the environment according to its radio range. The designing issue is to prolong the network life time and securily collect the data by mobile sink. Each of these mechanisms can achieve certain level of security and energy efficient data collection in the mobile sink wireless sensor networks. MSWSN takes into consideration because the communication and computation limitations of sensor node.

There is always a tradeoff between security and performance, experimental results. Here we proved that the proposed framework can achieve energy efficient routing and high degree of security with negligible overheads.

3.2 Proposed Data Collection Method

We consider there are n numbers of static homogenous sensor nodes placed uniformly in a square region given by a geographical area, for sensing data or monitoring events. Single mobile sink travers in the squared monitored region to collect data by one hop communication. It follows the proposed mobility model to travel through the service area to collect data. Sink collects the data from the sensors; those are within the radio range of the sink. It follows one hop data collection process. Data collection takes place in three step process. There are two types of data collection; one is proactive data collection and another is reactive data collections. In proactive data collection method sensed data distributed and store throughout the network for later retrieval of sink. In reactive data collection method data send to the sink after detection of sinks presence or query. Our model follows the reactive data collection. Figure 3.1 shows the sequence diagram of data collection.

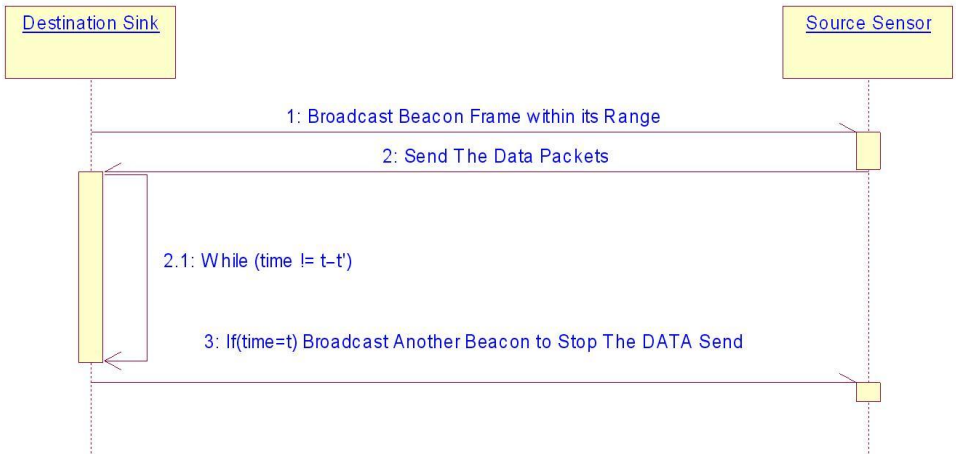

Figure 3.1: Sequence diagram of communication between sensor and sink.

During one hop data collection it performs with three step process, as shown in the sequence diagram. We need to specify the initial position of the sink. After that sink movement is based upon the proposed mixed mobility model. With following this mobility model sink changes its position and each new position it performs data collection operation with three step process. In first step, sink broadcast a new beacon frame to alert the sensors within its range for sink's presence. In second step, after proper identifying the sink node sensors send their sensed data to the sink. In last step, before sink changes position it broadcast a new beacon frame to alert the sensors within its range to stop the data transmission. we follow the last step to reduce the packet drop.

In Algorithm 1 initially sink starts motion from the initial position of the bounded services area. Sink changes its relative position according to the proposed mobility. Sink broadcasts a start beacon frame to the neighbor nodes. After receiving the beacon frame each sensor node set their value and starts to send the data packets to the sink till receives the stop beacon frame. Just before sink changes its position $(T - \delta T)$ time sink broadcasts another beacon frame to reset the neighbor nodes and stop the transmission, to reduce the packet drop. After that sink changes to a new position and follow the same procedure every time.

Algorithm 1

t= Current time

T= Simulation time //End time of the program

τ= Pause time //Remain same throughout the program

p(x, y) = Position of the sink

b_cast(id, start/stop) = Beacon frame broadcast by the sink.

1: initial_position$_{sink}$ = p(x, y)
2: $z \leftarrow \tau$
3: $t \leftarrow 0$
4: **repeat**
5: Sink= b_cast(id, start)
6: **while** (t $\leq z - \delta\tau$) **do**
7: Sink= recv_data(packets)
8: **end while**
9: **if** (t $\geq z - \delta\tau$) **then**
10: Sink= b_cast(id, stop)
11: **end if**
12: new_position$_{sink}$ = p(x′, y′)
13: $z \leftarrow t + \tau$
14: **until** (t = T)

3.3 Energy Consumption Model

The lifetime of sensor network depends on the operation time of individual sensor nodes. Therefore, a model, which defines the amount of power consumed in each action of a sensor node, influences the lifetime of networks to a great degree. In proposed work, we assume a model where the radio dissipates E_{elec}= 50nJ/bit to run the transmitter or receiver circuitry and ε_{amp}= 100pJ/bit/m^2 for the transmit amplifier to achieve an acceptable E_b/N_o [37].

The power needed to transmit k bits of data over a distance d is:

$$E_{tx} = E_{elec}k + \varepsilon_{amp}kd^2 \tag{3.1}$$

And the power needed to receive k bits of data is:

$$E_{rx} = E_{elec}k \tag{3.2}$$

Where d is the distance between the source and sink. Using a direct communication protocol, each sensor sends its data directly to the base station. If the base station is far away from the nodes, direct communication will require a large amount of transmit power from each node. This will quickly drain the battery of the nodes and reduce the network lifetime. Nodes route their packets to the base station through intermediate nodes. Thus nodes act as routers for other nodes in addition to sense the environment. The existing routing protocols consider the energy of the transmitter and neglect the energy dissipation of the receiver in determining the routes in Equation (3.2).

Depending on the relative costs of the transmit amplifier and the radio electronics, the total energy expended in the system might be greater in multi-hop transmission than direct transmission to the base station.

Assume that there are 'n' numbers of intermediate nodes to reach at the destination and also each adjacency nodes are differentiated with distance 'r' between them. So the total distance between source to sink is 'nr'. If we consider the energy expenditure at each node during transmitting a single k-bit message from source node 'N' to base station. A node located with a distance from the base station using the direct

communication approach is in equations 3.1 and 3.2, then from equation (3.1)

$$\begin{aligned} E_{direct} &= E_{Tx}(k, d = n * r) \\ &= E_{elc} * k + \varepsilon_{amp} * k * (nr)^2 \\ &= k(E_{elc} + \varepsilon_{amp} n^2 r^2) \end{aligned} \tag{3.3}$$

Packet passes through the 'n' intermediate nodes to reach at the destinations means it required 'n' times transmit and 'n-1' time receive. From Equation (3.2)

$$E_{rx} = (n-1)E_{elec}k \tag{3.4}$$

So total energy conservation to reach at the destination is

$$\begin{aligned} E &= n(E_{elc} * k + \varepsilon_{amp} * k * r^2) + (n-1)E_{rx} \\ &= E_{elc} * k * n + \varepsilon_{amp} * k * n * r^2 + (n-1)E_{elec}k \\ &= k((2n-1)E_{elec} + \varepsilon_{amp} n r^2) \end{aligned} \tag{3.5}$$

In the direct communication with base station the energy conservation is

$$\begin{aligned} E &= E_{tx} + E_{rx} \\ &= E_{elec}k + \varepsilon_{amp} k d^2 + E_{elec}k \\ &= E_{elec}k + \varepsilon_{amp} k r^2 + E_{elec}k \\ &= k(2E_{elec} + \varepsilon_{amp} r^2) \end{aligned} \tag{3.6}$$

From the above equations the total energy at n hop distance from the source to sink is defined in equation (3.5) and for single hop communication in equation (3.6).

3.4 Simulation Analysis

In this section we evaluate the performance of the proposed model and compare it with the existing technology with static network. The experiment has been done in ns 2.34, we have taken 100 random sensor nodes in the 1000x1000 meter area. Initially all sensor nodes have same level of enegy, i.e., 1 joule and the communication range 25 meters. The transmitting and receiving energy is 50 nJpb and transmit amplifier to achieve an acceptable form is 100pJpb.

Here we compared our proposed model Mobile Sink Wireless Sensor Networks (MSWSN) with traditional protocol flooding and flat routing protocol Sensor Protocol for Information via Negotiation (SPIN). SPIN is a negotiation base multi cast routing protocol [26]. Source first negotiates among the neighbors before start the data transfer.

Communication overhead becomes main issue in this type of network, which tends to MAC sub layer. Sensors transmit the packets to the sink node and sink collect it with CDMA protocol in our simulation model.

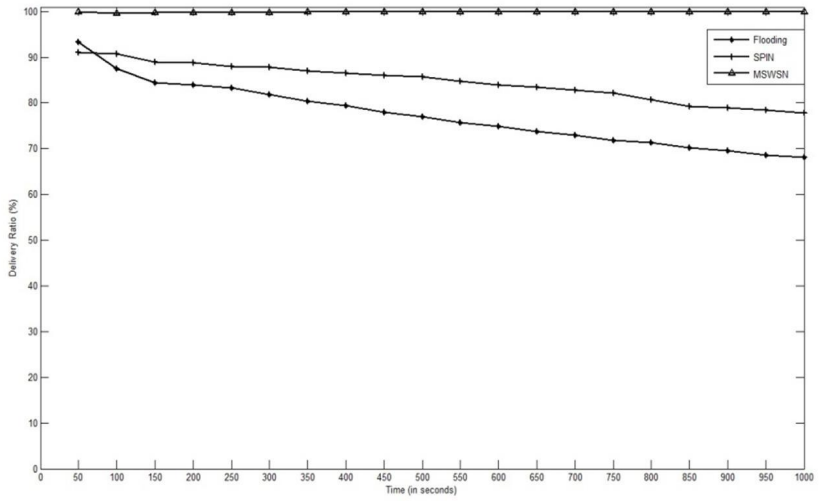

Figure 3.2: Delivery Ratio vs Time

In this Fig. 3.2 we have shown the delivery ratio of three routing protocols. Initially in flooding delivery ratio is higher than the SPIN because of their redundant data delivery nature. As soon as node dies, delivery ratio decreases. In SPIN the difference of minimum and maximum delivery ratio is less as compared to flooding. In the proposed model delivery ratio is nearly 100

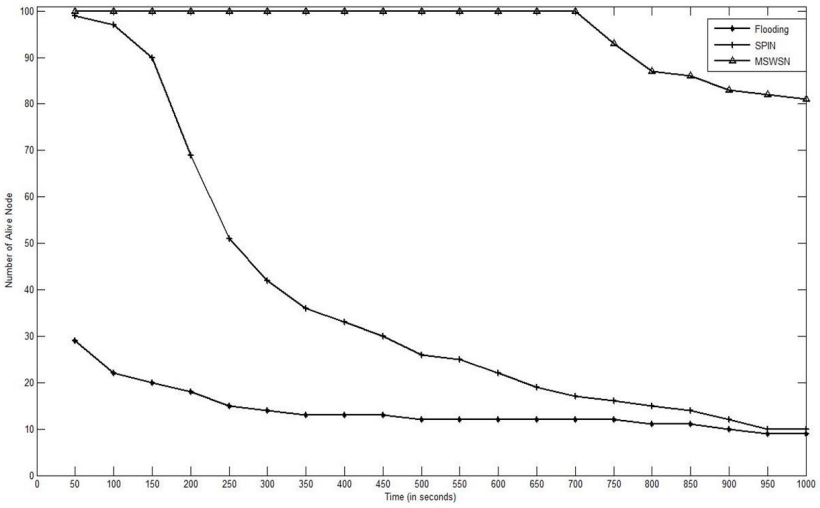

Figure 3.3: Number of alive node vs Time

Fig. 3.3 shows the comparison between the simulation time various alive node in the network. Because of the high complexity in flooding, nodes dies very quickly, hence many nodes die on the network, but the rate of dead node reduces during the simulations. In SPIN the dead node increases linearly, SPIN first negotiate with the neighbors before it sends data. In the proposed model for a long duration of simulation, network is stable. After a long time the rate of dead node increases linearly.

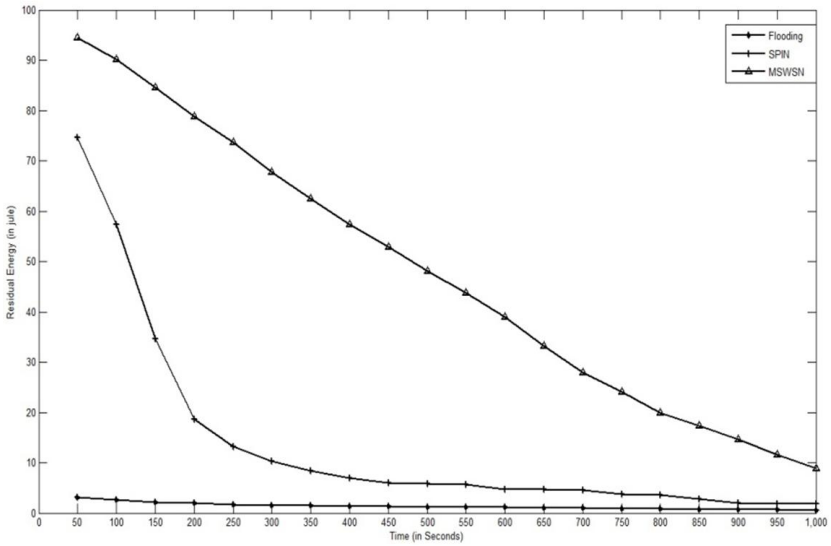

Figure 3.4: Residual Energy vs Time

Fig. 3.4 shows at initially of simulation residual energy of the network is very less

in flooding. The reason behind the drastic decrement of residual energy of the network is the broadcasting nature of the node. A large number of nodes die because of this resion and further the network becomes disconnected. That's why the residual energy of the network is almost constant till the end of the simulation. In SPIN during the simulation it transmits with negotiation based in order to reach at the destination. When a node reduces its energy below threshold level, it is not going to participate in data transmission. So that the decrement in the residual energy become almost constant in the rest of the experiment. Unlike SPIN, MSWSN doesn't require any path finding to communicate, which decreases the residue energy linearly.

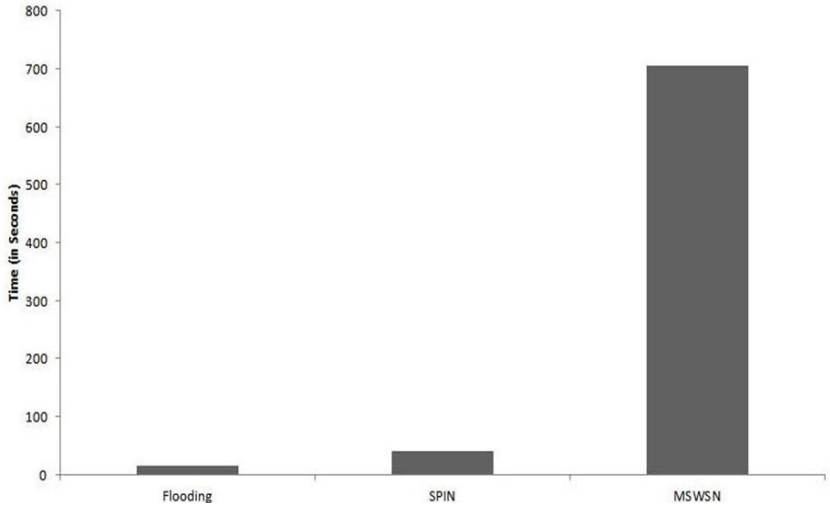

Figure 3.5: First node dies in the network

Network life time means the first node dies in the network. Fig. 3.5 shows the First 12node dies in the network with considering various technologies. In flooding the first node dies very quickly in the considering scenario because it floods the data packets to entire network in-order to deliver the data packets. Comparatively flooding, SPIN saves more energy and sends the data to the destination. It sends the data after establishes the path and follow the same path until it breaks. In this way the node dies slowly. In the MSWSN model more energy saves and all nodes of the network are alive for long period of time.

3.5 Secure Communication During Data Collections

We use symmetric key cryptography because asymmetric cryptography use different key for encryption and decryption. Asymmetric key is computationally high. Sensor node have limited computational resources, so asymmetric key cryptography is not appropriate for sensor networks. Symmetric key uses single secret key for both encryption and decryption. As resource constraints in sensor node symmetric key is appropriate for the Wireless Sensor Networks. Here we use symmetric key cryptography to encrypt the data and authenticate the node. We assumed sink has no resource limitation, so take sink as the centralize controller.

Assumptions

Sensor node's secret key —k_i

Sink node's secret key —k_s

Shared key —k_{sh}

Large prime number —p_i

CAC —Central Authentication Code

SAC —Sensor Authentication Code

MAC —Message Authentication Code

H()—Hash function to calculate hash value

Node's Operations

Sink's operation:

$CAC = H(E(p_i, k_s))$

$DATA = C_D \oplus CAC \oplus k_i / DATA = C_D \oplus SAC$ (decrypt the cypher text to get the original data)

Sensor's operation:

$SAC = CAC \oplus ki$

$CD = DATA \oplus SAC$ (encrypt the plain text with secret key)

Procedure for node authentication:

Algorithm 2 Operation at Sink

1: After a fixed amount of time sink generates a random large prime number (p_i) and calculates CAC = H(E(p_i, k_s))
2: Distribute the *CAC* among the networks
3: Broadcast the beacon frame with containing $k_{sh} \oplus k_s \oplus$CAC
4: Receive the cipher text message Cd and decrypt it with own scret key DATA = $C_D \oplus$ CAC$\oplus k_i$
5: Compare the DATA with the MAC if it same *accept* else*reject*
6: If DATA packet is rejected then sink send a *NAK* to corresponding sensor to resend.
7: Go to the *step.4* till end of the pause time.

Algorithm 3 Operation at Sensors

1: Each sensor calculate its own secret key with receiving the *CAC* from sensor SAC = CAC$\oplus$ki
2: When it receive the broadcast it check it with B_cast$\oplus$CAC$\oplus k_{sh}$ If result is same as sink secret key then accept else reject.
3: Sensor encrypts its data with own secret key to generate cypher text CD = DATA$\oplus$ SAC
4: Append the MAC at the end of the packet for verification.
5: Go to *step.3* till end of pause time or no more data to send.

In our proposed method, in regular interval of time sink generates a large prime number. It produces Central Authentication Code (CAC) by hash the value after encrypting the prime number with sink secret key (k_s) [42]. Then distribute the CAC in the network. All sensors in the service area calculate Sensor Authentication Code (SAC) by ex-or the CAC with sensor secret key (k_i). Sink node broad cast the packet with shared key, sink secret key and CAC (B_cast = $k_{sh} \oplus k_s \oplus$CAC). Sensors receive the packets and decrypt the packets with the operation B_cast$\oplus$CAC$\oplus k_{sh}$. Sensors accept the packet after checking the authentication of sink. If it accepted sensor send the data

packets encrypting with SAC to produce cipher text of the data (C_D) and continue the process till no data packets to send or end of the sink's pause time. Sink receive the packets with decrypting the packets with this process DATA = $C_D \oplus CAC \oplus k_i$. Then compare the DATA with the MAC, if this same sink accept the packet otherwise reject. Figure 3.6 shows the communication between the sensor and sink.

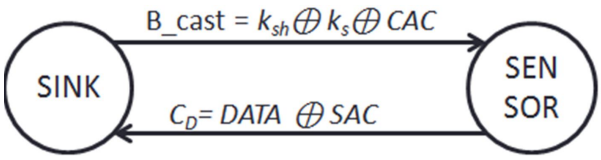

Figure 3.6: Communication between sensor and sink

3.6 Security Analysis and Performance Comparison

At the Network Initialization phase, each node stores a set of secret keys, shared key and an authenticator operator. Taking into account the typical number of neighboring nodes in this kind of networks [40] and the key length we are considering (128 bits), the memory storage wants of the proposed scheme appear as follows.

For example, for the node density of 5 neighbors, key length of 128 bits, 160-bits output hash function, and a 10 tuples authenticator, the required memory is about 360 bytes only.

Security properties required by mobile sink sensor networks include that data confidentiality, data authentication, data integrity, data freshness [32].

In our proposed key exchanged algorithm, we generate CAC with the hash function so that the malicious node can never hack it; we encrypt the DATA message with SAC to keep or get the data authentication; SAC is generated by Ki, it makes realize the data is confidential. With the privacy authentication technology, we set up secure channels between sensors and sink node with using the shared key concept.

In addition, we use MAC code to confirm data integrity; it makes the receiver believe that the received data is not modified during transmission by an adversary.

In our model, we use large prime number to keep data freshness. It ensures that

the data is recent, and it ensures that no adversary replayed old messages. So we here also ensure that each message is fresh. Sink generate a large prime number after fixed amount of time to keep data freshness and it also make confusion to adversary node.

We use the CDMA technology to improve secure communication because of that the CDMA can provide cheap, clear, and energy efficient wireless communication [43].

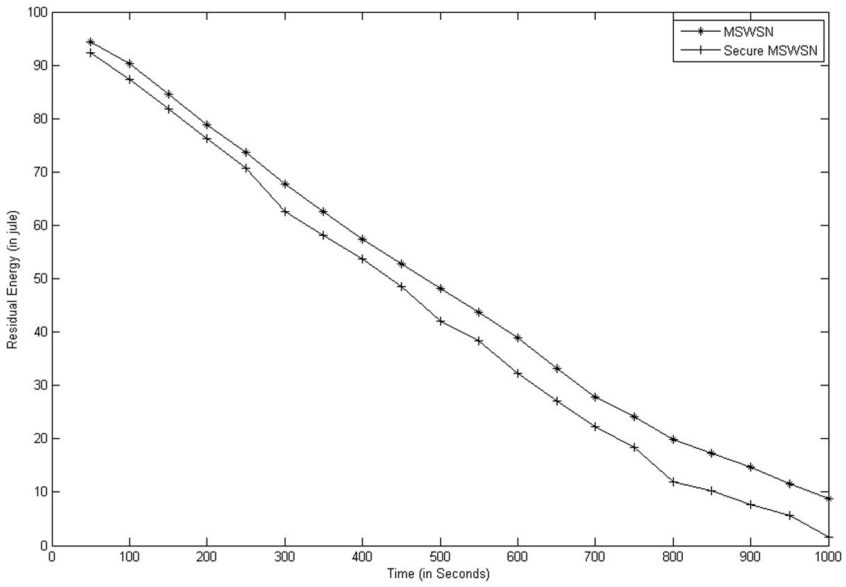

Figure 3.7: Residual energy of the network vs Time

Figure 3.7 shows the comparison between the mobile sink data collection and secure data collection with considering network residual energy. At initially simulation residual energy of the network is 100 jule. We have already implemented the mobile sink data collection technique and here it is compared with after applying the symmetric key cryptography for MSWSN. After a fixed amount of time it drastically changes the network energy because of the key updating by the sink and distribute among the network and each node calculate its own key.

3.7 Conclusion

This chapter, a new framework for energy efficient secure data collection is proposed. The proposed framework uses a new approach of one hop communication and node

authentication on the base of secure energy efficient algorithms for sensor networks. We have simulated the proposed model and compared with traditional protocol for static sensor networks. Here we use symmetric key cryptography for secure data collection. Communication between sensor nodes and the sink is secured as the sensor data is encrypted using symmetric key cryptography. In the propose scheme the large prime is generated in a fixed time interval of time to avoid replay attack and keep data freshness.

Chapter 4

Secure Protocol for Critical Data Transmission Towards Mobile Sink

Introduction

Working Model of SPIN

Mechanism Of Routing Towards Mobile Sink

Mathematical Model for Data Transmission

Simulation and Performance Analysis

Secured SPIN for Data Transmissions

Security Analysis

Conclusion

4.1 Introduction

Wireless sensor network is becoming an increasingly important technology that will be widely used in a variety of applications such as public safety, environmental surveillance, disaster surveillance, medical, home and office security, transportation, and military[1]. Routing protocol in sensor network is very pivotal. SPIN protocol is a basic data-centric routing protocol of wireless sensor networks [41]; though many new algorithms have been proposed for the problem of routing data in static sensor networks not for the mobile sink [45]. Our goal is to show that SPIN work efficiently for critical data transmission towards mobile sink and use symmetric key cryptography for secure data transmission to mobile sink.

In our proposed model sink is not static, it traverse network with random relative motion to collect the data. If sensor sense any critical data and sink is not in its range for that situation sensor needs to send its data immediately toward mobile sink. As sink is moving randomly in the network, the traditional protocol proposed for static network can't work. For that, sensor needs to flood the data to reach at the destination. SPIN protocols can deliver 60% more data for a given amount of energy than conventional approach [41]. Here mathematically in Equation 4.3 proved that it doesn't take the extra cost for the mobility of the sink node.

Sensor Network mainly deployed for risk management like disaster surveillance, environmental surveillance and military etc. So we need to route the critical data to sink, which will transfer the data to the base station immediately.

4.2 Working Model of SPIN

The performance of SPIN is better than of flooding, gossiping and ideal protocol for energy and bandwidth consumption [41]. These three protocols function comparisons as: (i) flooding, which broadcast the packet among all of its neighbors; (ii) gossiping, a variant on flooding that sends messages to random sets of neighboring nodes; and (iii) ideal, an idealized routing protocol that assumes perfect knowledge and has the

best possible performance.

The traditional protocols which establish a path before transmit the data are also not suitable for the mobile sink. Because each time sink is changes its position. It needs to flood the data in order to reach at the sink node.

Sensor Protocol for Information via Negotiation Protocol (SPIN) has four types: SPIN-PP, SPIN-EC, SPIN-BC, and SPIN-RL [41]. In our work, we consider SPIN-EC as the best protocol. In SPIN-PP, Nodes use three types of messages ADV, REQ and DATA to communicate [3]. When energy is plentiful, SPIN-EC nodes communicate using the same three-stage protocol as SPIN-PP nodes. When a SPIN-EC node observes that its energy is approaching a low-energy threshold, it adapts by reducing its participation in the protocol. ADV is used to advertise new data, REQ is also to request for data and DATA is the actual message. The protocol starts when a SPIN node gets new data that it is willing to share on on-demand basis. It does so by broadcasting an ADV message containing meta-data. Meta-data size is very small as compared to the size of the DATA. If a neighbor is interested in the data, it sends an REQ message for the DATA and the DATA is sent back to this neighbor node. The neighbor sensor node then repeats this process to its neighbors till reach at the sink node.

Figure 4.1 [41] shows an example on how this protocol works. It starts by advertising its data to node B from Node A(a). Node B responds by sending a request to node A (b). After receiving the requested data (c), node B then sends out advertisements to its neighbors (d), who in turn send requests back to B (e, f).

The strength of this protocol lies in its simplicity. Each node in the network performs little decision making when it receives new data, and therefore wastes little energy in computation. Furthermore, each node only needs to know about its single-hop network neighbors.

4.3 Mechanism Of Routing Towards Mobile Sink

Our work mainly focused on mobile sink wireless sensor networks, where all the sensors are static in nature. Only the sink node dynamically changes its position.

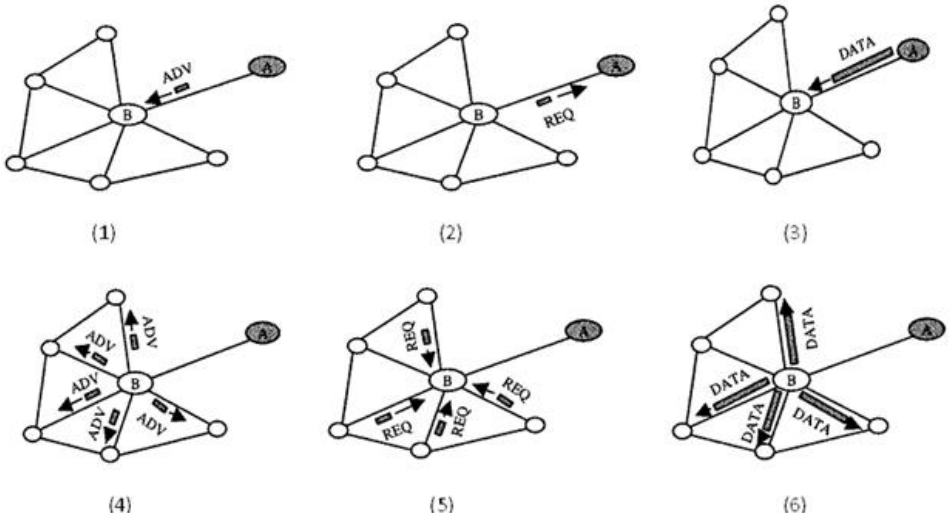

Figure 4.1: The SPIN-PP protocol [41].

Mobility is restricting within the sensing bounded area. Which is a cause to the prolog of network lifetime. Our intension is to show how efficiently SPIN can work in the mobile sink WSN.

In our assumption all nodes are static other than the sink node. Sink node moves randomly in the field. The position, speed and direction calculates randomly in Equation 2.1, 2.2, 2.3 after each step of moving.

According to SPIN characteristics, sensors communicate with the sink via negotiation. When sensor node starts send the data to the sink node, each time it finds the path following negotiation based approach to reach at sink as described above. Because SPIN protocol doesn't establish the path to the sink node while going to send. It is a three step process to communicate with sink node.

Figure 4.2 shows the data transmission to the mobile sink according to the SPIN characteristics. Here K_1 to K_6 are the static nodes and S is the mobile sink node. Form figure 4.2 node k_1 sends the packet to the sink node when it is at P_1 and deliver the data to the sink when it is at the position P_2. Sink move from the position P_1 to P_2 during the data transmission.

SPIN is the better protocol then those traditional protocols which first establish the path then transmit the data to sink. In this situation sink always changes the position

dynamically as derived in the Equation 2.1, so it is not feasible to establish the path and follow to transmit the data to the sink. As per the mathematical derivation Equation 4.3 SPIN works efficiently in mobile sink WSN. Which proved in the next Section-IV and it is better than the flooding, gossiping and ideal protocol for energy and bandwidth consumption [41].

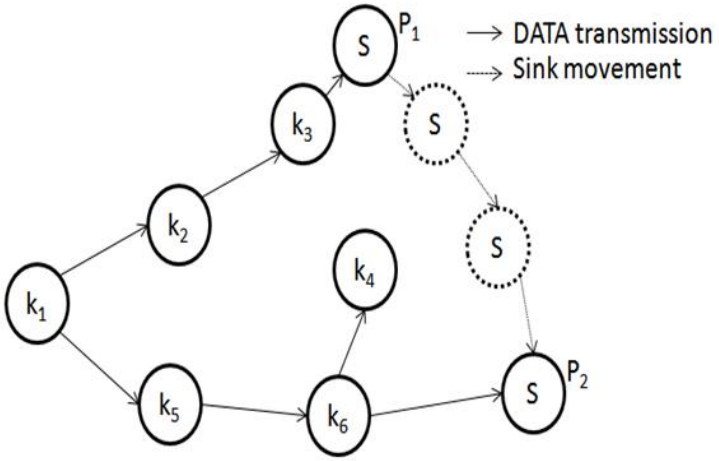

Figure 4.2: Data transmission with mobile sink.

4.4 Mathematical Model for Data Transmission

Figure 4.3 shows the data transmission to the sink when sink at the P_1 hop distance from source (a) and P_2 hop distance from source (b). Source starts to send the data with multicasting according to the SPIN property. Each time it starts with the greedy incremental tree (GIT) to reach at the sink.

Each node in the tree (except the sink) makes the transmission till reach at the sink. So GIT starts from source node.

In this case number of transmission is equal to number of edge of the tree. And number of the edge of the tree is the cost for transmission.

Assumed that, the distance from source to sink is D_x, cost to transmit the data with distance D_x is C_x and each node can disseminate the maximum 'n' number of packets.

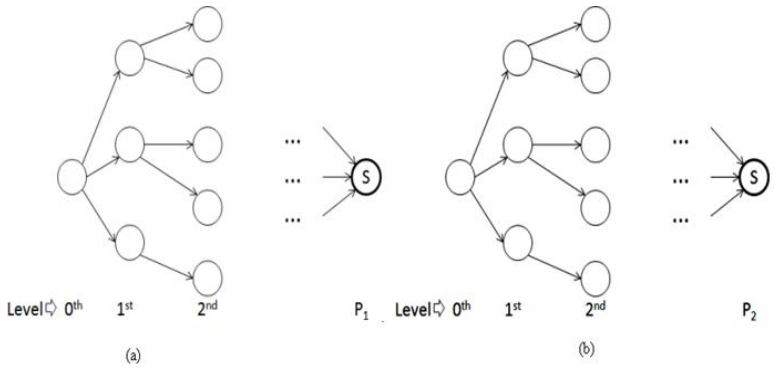

Figure 4.3: Transmission of data when sink is (a) at P_1 hop distance (b) P_2 hop distance from source.

When sink is at position P_1.shown in Figure 4.3(a), the maximum number of packet dissemination to reach at the sink node at distance:
Can be formulated as

$$C_1 = \frac{n^{p_1} - n}{n-1} + k \tag{4.1}$$

Where k < n, number of packets transmit at last step to reach at the sink.

For the distance (D_1) is directly proportional to cost

i.e $D_1 \propto C_1$

Similarly at the position of sink at P_2 is $D_2 \propto C_2$;

In general

$$D_x \propto C_x \tag{4.2}$$

Cost depends on distance between the sources and sink node not the position and the direction. Here it shows the position means the distance of sink position from the source node. This shows the following equations;
i.e. $p(x_1, y_1)$ = distance form sink to position (x_1, y_1)

if $P(x_1, y_1) > P(x_2, y_2)$
then $D_1 > D_2, C_1 > C_2$,
if $P(x_1, y_1) < P(x_2, y_2)$
then $D_1 < D_2, C_1 < C_2$,
and if $P(x_1, y_1) = P(x_2, y_2)$

then $D_1 = D_2, C_1 = C_2$

Thus the increase in delay is approximately proportional to:

(Distance between farthest source and sink) − (Distance between closest source and sink) (4.3)

Cost depends on distance between source and sink, not on the directions and speed using the SPIN protocol.

4.5 Simulation and Performance Analysis

In this section we evaluate the performance of the protocol proved for MSWSN and compare it with the traditional flooding technique. The experiment has been done in ns 2.34, we have taken 100 random sensor nodes in the 1000×1000 meter area, a sparse network. Initially all sensor nodes have same level of enegy, i.e., 1 joule and the communication range 25 meters. The transmitting and receiving energy is 50 nJpb and transmit amplifier to achieve an acceptable form is 100pJpb. Here we assumed the simulation parameter as previous one.

Communication overhead becomes main issue in this type of network, which tends to MAC sub layer. Sensors transmit the packets to the sink node and sink collect it with Selective CDMA protocol in our simulation model.

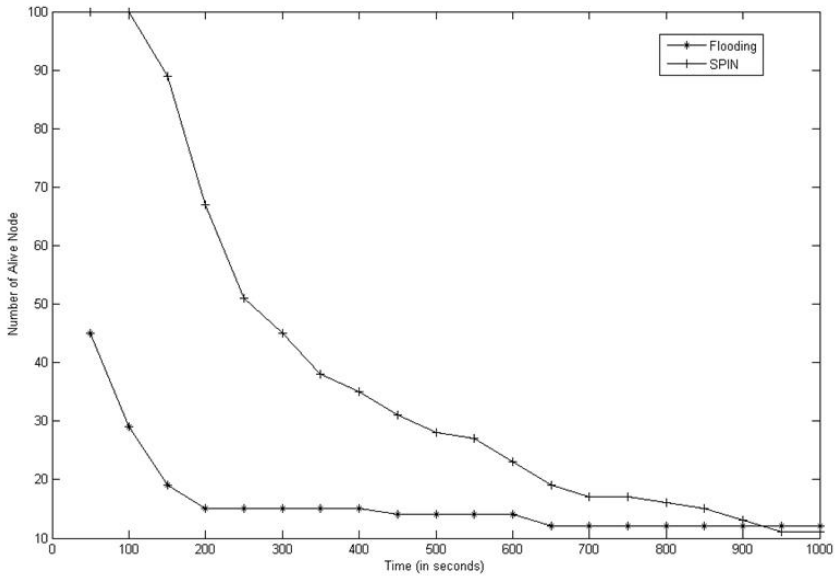

Figure 4.4: Number of alive node vs Time

Figure 4.4 shows the comparison between the simulation time versos alive node in the network. Because of the high complexity in flooding, nodes dies very quickly, hence many nodes die on the network, but the rate of dead node reduces during the simulations is very quickly. In SPIN the dead node increases linearly, SPIN first negotiate with the neighbors before it sends data. So maximum numbers of nodes are alive in the network and deliver the more data towards mobile sink.

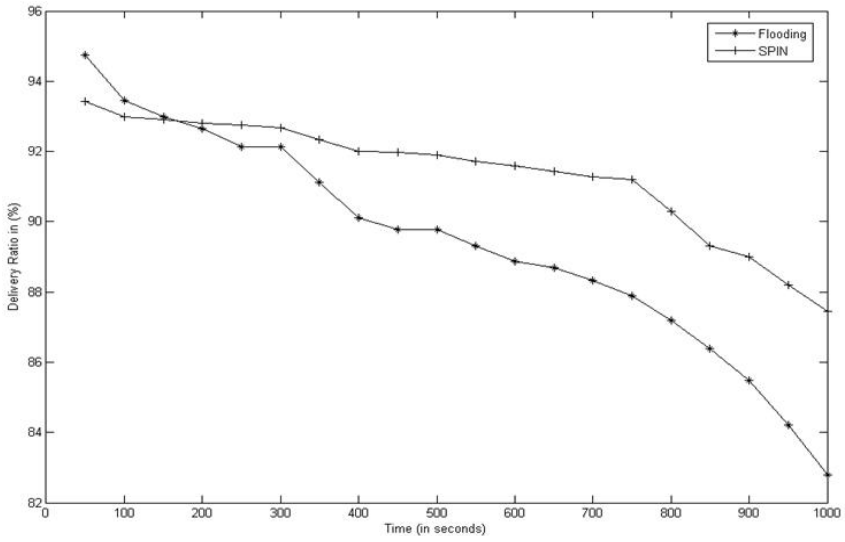

Figure 4.5: Delivery ratio vs Time

In the Figure 4.5 we have shown the delivery ratio towards mobile sink. Initially in flooding delivery ratio is higher than the SPIN because of their redundant data delivery nature. As soon as node dies, delivery ratio decreases. In SPIN the difference of minimum and maximum delivery ratio is less as compared to flooding. Initially it delivers less packets compared to flooding and after a certain period SPIN delivers more data towards mobile sink.

4.6 Secured SPIN for Data Transmissions

We use the same assumption/ keys used in previous for the data encryption and confidence. We use the same symmetric key cryptography for data encryption and decryption. Symmetric key uses single secret key for both encryption and decryption. Each sensor has it's secret key and a shared key for data encryption and authentication. As we assumed sink has no resource limitation, sink is taken as the centralize controller. Sink node also have its secret key and all sensors secret key. As resource constraints in sensor node symmetric key is appropriate for the Wireless Sensor Networks.

Sensor use SPIN protocol for critical data transmission towards mobile sink in MSWSN. Here we use symmetric key cryptography for data encryption during transmission.

4.6.1 Assumptions

Sensor node's secret key —k_i

Sink node's secret key —k_s

Shared key —k_{sh}

Large prime number —p_i

CAC —Central Authentication Code

SAC —Sensor Authentication Code

MAC —Message Authentication Code

H()—Hash function to calculate hash value

4.6.2 Procedure

During network initialization the secret key and shared key distributed among all nodes in the network. Sink generates a large prime number in a fixed time interval. Each time it generates a new key, using that large prime number, *CAC* (Central Authentication Code) by CAC = H(E(p_i, k_s)) as described in the previous chapter and distribute throughout the networks [42]. After getting this CAC, sensors update their key with generating *SAC* (Sensor Authentication Code) SAC = CAC$\oplus k_i$. Sink updates with this large prime number to avoid replay attack and keep data freshness.

At *ADV* message sending phase, the node which have critical data send to sink that should encrypt the *ADV* with the shaired key to avoid an external attacker. As per Figure 4.1, if node A wants to send its data, it first encrypts *ADV* with its shared key k_{sh} to get an encrypted ADV, and then send the encrypted *ADV* to all its neighbors. Those sensors get the *ADV* packet it decrypt with the shared key to get the ADV. It trusts that *ADV* comes from the legitimate node if it can able to decrypt the *ADV* using shared key. Then the sensor checks to see if it possesses all of the advertised data. If not, it sends an *REQ* message back to node A, asking for the data it would like to acquire.

At *DATA* message sending phase, if a sensor node wants to send data to sink, it first XOR data with its SAC, then adds *MAC* at the end of the packet [43], and then sends the packet to sink via its own CDMA [43] code. Only sink can decrypt the data packets with its key and sensor's secret key. To decrypt the *DATA* sink first pulls out the respective K_i, using K_s, the sink checks *MAC* to see if the data is altered. If there is no alteration, then the sink XOR the coming data with K_i and current *CAC*. Result is the original data sent by the sensor node.

4.7 Security Analysis

Security properties required by mobile sink sensor networks include that data confidentiality, data authentication, data integrity, data freshness [32].

In our proposed key exchanged algorithm, we generate *CAC* with a hash function

so that the malicious node can never hack it; we encrypt the *DATA* message with *SAC* to keep the data authentication; *SAC* is generated by K_i, it makes realize the data is confidential. With the privacy authentication technology, we set up secure channels between sensors and sink node with using the shared key concept. Sink generate a large prime number after fixed amount of time to keep data freshness and it also make confusion to adversary node. In addition to this *MAC* is used for data integrity, it confirms the receiver that the received data is not altered in transit by an adversary.

In our model, we use large prime number to keep data freshness. It ensures that the data is recent, and it ensures that no adversary replayed old messages. So we here also ensure that each message is fresh.

We use the CDMA technology to improve secure communication because of that the CDMA can provide cheap, clear, and energy efficient wireless communication [43].

4.8 Conclusion

In this chapter, we proved an existing protocol SPIN is appropriate for data transmission towards mobile sink. Which is more energy efficient than the general flooding technique. We use symmetric key cryptography for secure data transmission to wards mobile sink. We have implemented the security using symmetric key cryptography to avoid external attack and keep data freshness. We simulated the protocol and compare the performance for energy conservation and delivery ratio. In next session we analyze the security for secure protocol. Here sink uses large prime number after generating a fixed amount of time to keep data freshness and avoid the external attack. Intermediate sensors only authenticate the other senosrs during data transmission and only authorised sink can decrypt the data packets.

Chapter 5

Conclusion and Future Work

Conclusion

Future Work

5.1 Conclusion

In this thesis we proposed a method for data collection to prolong the network lifetime and session based symmetric key cryptography in mobile sink sensor networks. In our algorithm we provide security and energy efficiency method for data collection. There are several static methods are available for this which uses different approaches to provide security in resource limited wireless sensor networks. In mobile sink based approaches, sink travers the network randomly and data collection from single hop sensors. Sinkt have enough energy, memory and computational power. We exploited this approach and proposed a new mechanism for secure data collection which can able to avoid external attack and authenticate the node during the data collection process.

The proposed security method provides positive features of symmetric key cryptography. Proposed method provides the security features with reducing the packet drop and keep data freshness. In this method sink generate a large prime number after a fixed period of time to keep data freshness and avoid the replay attack. With using the shared key sink broadcast the message at each position. Sensors authenticate sink with using their shared shared key. Then sensors send the packet encrypted with their secret key.

For the critical data transmission to mobile sink we proved an existing protocol (SPIN) is suitable for mobile sink. We use symmetric key cryptography for secure data transmission towards mobile sink. Proposed method can able to avoid the external attack and authenticate the intermediate node while transmitting towards mobile sink.

Our analysis of comparison results established that our proposed method is secured and provide better performance.

5.2 Future Work

To conclude this thesis, following are some points that may lead to some betterand interesting results.

IEEE 802.15.4-based mobile sink wireless sensor network has a lot of security threats

because it has very low computational power and limited resources [47]. Such threats can be classified by network layering architecture such as jamming and tampering in physical layer, collision, exhaustion, unfairness in link layer, spoofed, altered or replays routing information, selective forwarding, sinkhole and wormhole in network layer, flooding and desynchronization in transport layer. The security suites consists of 8 different security levels, and each level means a kind of cryptographic algorithm, the mode of block cipher, message authentication code, and the size of message authentication code [48, 49]. Our work can be further extended to satisfy these different security levels.

There are seven security requirements namely: availability, authorization, authentication, confidentiality, integrity, non-repudiation, and freshness [47]. In this thesis we have addressed to keep only node authentication, data freshness during data collection. It can be further enhanced to satisfy the other security requirements. While applying the security framework, it needs to consider energy consumption because of the limited power of sensor nodes.

For the critical data transmission towards mobile sink in Mobile Sink Sensor Networks the SPIN protocol can be further improvised for energy efficient data transmission towards mobile sink. Security models can be improvised to avoid several internal attack like sink hole, wormhole, replay and sybilattacks which are arises during critical data transmissions.

Bibliography

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, Volume: 40 Issue: 8, pp. 102- 114, August 2002.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks vol. 38, pp. 393- 422, 2002.

[3] Ismail H. Kasimoglui and Ian .F. Akyildiz, "Wireless Sensor and Actor :Research Challenges," (Elsevier) Journal, vol.38, no.2, pp. 351-367, 2004.

[4] Sungha Pete Kim, Bo-Cheng Charles Lai, David D. Hwang and Ingrid Verbauwhede, "Reducing radio energy consumption of key management protocols for wireless sensor networks," Proceedings of the 2004 International Symposium on Low Power Electronics and Design, pp. 351- 356. Aug. 2004.

[5] Prasan K. Sahoo, J. Jen-Rong Chen and Ping-Tai Sun, "Efficient security mechanisms for the distributed wireless sensor networks," Proceedings of the IEEE Third International Conference on Information Technology and Applications (ICITA'05), pp. 541- 546 vol.2, July 2005.

[6] R.K. Ghosh, Vijay Garg, M.S. Meitei, S. Raman, A. Kumar and N. Tewari, "Dense cluster gateway based routing protocol for multi-hop mobile ad hoc networks," Ad hoc networks. pp. 168-185, 2006.

[7] P.Nair, H.Cam, S.Ozdemir and D. Muthuavinashiappan, "Espda: Energy efficient and secure pattern based data aggregation for wireless sensor networks," Computer Communications IEEE Sensors, pp. 732- 736, Oct. 2003.

[8] J. Stankovic A. Perrig and D. Wagner, "Security in wireless sensor networks," Communications Of The Acm, Vol. 47, No. 6, pp. 53-57, June 2004.

[9] G.J. Pottie and W.J. Kaiser, "Wireless integrated network sensors," Communications of the ACM vol.43, issue 5, pp. 551-558, may 2000.

[10] J.M. Rabaey, M.J. Ammer, J.L. da Silva Jr., D. Patel and S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking," IEEE Computer Magazine, vol. 33, issue 7, pp. 42-48, july 2000.

[11] A. Ashraf, A. Rauf, M. Mussadiq, B. S. Chowdhry and M. Hashmani "A model for classifying threats and framework association in wireless sensor networks," 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, pp. 7-9, August 2009.

[12] J. Yick, B. Mukherjee and D. Ghosal "Wireless sensor network survey," Computer Networks vol.52, issue 12, pp. 2292-2330, Aug. 2008.

[13] Hiren Kumar Deva Sarma and Avijit Kar "Security Threats in Wireless Sensor Networks,"in Proceedings of 40th Annual IEEE International Carnahan Conferences Security Technology, pp. 243 - 251, Oct. 2006.

[14] John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary "Wireless Sensor Network Security: A Survey," Auerbach Publications, CRC Press, Jul. 2006.

[15] D. W. Carman, P. S. Krus and B. J. Matt "Constraints and approaches for distributed sensor network security," Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[16] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "Spins: security protocols for sensor networks," Wireless Networking, vol. 8, issue 5, pp. 521-534, 2002.

[17] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41-47. ACM Press, 2002.

[18] J Luo and J. P HUBAUX, "Joint mobility and routing for lifetime elongation in wireless sensor networks, " In Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM'05). Vol. 3. pp. 1735-1746, 2005.

[19] Wendi B. Heinzelman, Amy L. Murphy, Hervaldo S. Carvalho and Mark A. Perillo, "Middleware to Support Sensor Network Applications," IEEE Network, pp. 6-14, 2004.

[20] I. Papadimitriou and L. Georgiadis, "Energy-aware routing to maximize lifetime in wireless sensor networks with mobile sink," J. Comm. Softw. Syst. 2, pp. 141-151, 2006.

[21] J. Luo, J. Panchard, M. Piorkowski, M. Grossglauser and J-P Hubaux, "MobiRoute: Routing towards a Mobile Sink for Improving Lifetime in Sensor Networks," 2nd IEEE/ACM Intl Conf. on Distributed Computing in Sensor Systems (DCOSS), pp. 480-497, 2006.

[22] A. Chakrabarti, A. Sabharwal and B. Aazhang, "Using Predictable Observer Mobility for Power Efficient Design of Sensor Networks," in the proceeding of second International Workshop on Information Processing in Sensor Networks (IPSN), pp. 129-145, 2003.

[23] Arun A. Somasundara, A. RamamoorthY and M B. Srivastava, "Mobile element scheduling with dynamic deadlines," IEEE Transactions on Mobile Computing, vol. 6, No. 4, pp. 395-410, April 2007.

[24] M. Ma and Y. Yang, "SenCar: An energy-efficient data gatheringmechanism for large-scale multihop sensor networks," IEEE Transactions on Parallel and Distributed System vol. 18, No. 10, pp. 1476-1488, oct 2007.

[25] G. Xing, T. Wang, Z. Xie and W. Jia, "Rendezvous planning in wireless sensor networks with mobile elements," IEEE Transactions on Mobile Computing, vol. 7, No. 12, pp. 1430-1443, Dec 2008.

[26] J. Rao and S. Biswas, "Joint routing and navigation protocols for data harvesting in sensor networks," In Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 143-152, 2008.

[27] G. Xing, T. Wang, W. Jia and M. Li, "Rendezvous design algorithms for wireless sensor networks with a mobile base station," In Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'08), pp. 231-240, 2008.

[28] Li, Harnes, Holte, "Impact of Lossy Links on Performance of Multihop Wireless Networks," IEEE, Proceedings of the 14th International Conference on Computer Communications and Networks, pp. 303 - 308, Oct 2005.

[29] Yunxia Chen and Qing Zhao "On the Lifetime of Wireless Sensor Networks," IEEE communications letters, vol. 9, no. 11, pp. 976- 978, November 2005.

[30] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, pp. 189-199, 2001.

[31] Deepak Puthal, Bibhudatta Sahoo and Suraj Sharma, "Dynamic Model for Efficient Data Collection in Wireless Sensor Networks with Mobile Sink," International Journal of Computer Science and Technology, Vol. 3 Issue 1, pp. 623 - 628, March 2012.

[32] J. P. Hubaux, L. Buttyan and S. Capkun, "The quest for security in mobile ad hoc networks," ACM Symposium on Mobile Ad Hoc Networking and Computing, 2001.

[33] B. Liang and Z. Haas, "Predictive distance-based mobility management for PCS networks," In Proceedings of the Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), March 1999.

[34] M D Francesco, S K. Das and G. Anastasi "Data Collection in Wireless Sensor Networks with Mobile Elements: A Survey," ACM Transactions on Sensor Networks, Volume 8 Issue 1, 7:1-7:31, August 2011.

[35] Di Francesco M., Shah K., Kumar M., and Anastasi G. "An adaptive strategy for Energy efficient data collection in sparse wireless sensor networks," In Proceedings of the 7th European Conference on Wireless Sensor Networks (EWSN 2010), pp. 322-337 Feb. 2010.

[36] Deepak puthal and Bibhudatta Sahoo, "Adaptive Protocol for Critical Data Transmission of Mobile Sink Wireless Sensor Networks," in proceeding of IEEE International Conference on Computing, Communication and Applications (ICCCA-2012) India, Feb. 2012.

[37] R.Heinzelman, A. Chandrakasan and H.Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks," in Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), Maui, HI, pp. 3005-3014, Jan. 2000.

[38] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, IJCSIS, pp. 1- 9, Vol. 4, No. 1 and 2, 2009.

[39] Apostolos, Pyrgelis. "Cryptography and Security in Wireless Sensor Networks," [Presentation Slides] Greece : Department of ComputerEngineering and Informatics, 2009.

[40] Anderson R., Chan H. and Perrig A, "Key infection: Smart trust for smart dust," In Procroceding of 12th IEEE International Conference on Network Protocols (ICNP 2004), pp. 206-215, Oct. 2004.

[41] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.

[42] D. Xiao, M. Wei and Y. Zhou, "Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks," 1ST IEEE Conference on Industrial Electronics and Applications, pp. 1-4, 2006.

[43] H. Cam, S. Ozdemir, D. uthuavinashiappan, and P.Nair, "Energy-efficient security protocol for wireless sensor networks," IEEE VTC Fall 2003 Conference, pp. 4-9, Oct. 2003.

[44] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin and P . Corke, "Data Collection, Storage, and Retrieval with an Underwater Sensor Network," Proceedings of the 3rd international conference on Embedded networked sensor systems, ACM SenSys 2005.

[45] A. Rasheed and R Mahapatra, "An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks," ISSNIP 2007, p.p 703 - 708, Dec. 2007.

[46] M. Vecchio, A. Viana, A. Ziviani and R. Friedman, "DEEP: Density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility," Computer Communications, Vol. 33 Issue 8, pp. 929-939, May 2010.

[47] T. Shon, B. Koo, H. Choi and Y. Park, "Security Architecture for IEEE 802.15.4-based Wireless Sensor Network," 4th International Symposium on Wireless Pervasive Computing, 2009, pp. 1-5, 2009.

[48] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks," WiSe'04 Proceeding, pp.32-42, 2004.

[49] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta and Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", Computer Communications, Volume 30, Issue 7, Pp. 1655-1695, May 2007.

Dissemination of Work

Published:

- **Deepak Puthal** and Bibhudatta Sahoo, "Adaptive Protocol for Critical Data Transmission of Mobile Sink Wireless Sensor Networks" IEEE International Conference on Computing, Communication and Applications (ICCCA-2012) Dindigul, India, Feb. 22- 24, 2012.

- **Deepak Puthal**, Bibhudatta Sahoo and Suraj Sharma, "Dynamic Model for Efficient Data Collection in Wireless Sensor Networks with Mobile Sink" International Journal of Computer Science and Technology, Volume 3 Issue 1, pp. 623 - 628, March 2012.

Communicated:

- **Deepak Puthal** and Bibhudatta Sahoo "Symmetric key Based Secure Data Collection Method in Mobile Sink Wireless Sensor Networks" Ninth International Conference on Wireless and Optical Communications Networks (WOCN2012), Sept. 2012.